



OFFICE OF THE SECRETARY OF STATE

JESSE WHITE • Secretary of State

May 31, 2018

Rosa Escareno, Commissioner
City of Chicago
Department of Business Affairs and Consumer Protection
2350 West Ogden Avenue, Second Floor
Chicago, IL 60608

**Re: On-Line Access Agreement between the Illinois Secretary of State
and the City of Chicago, Department of Business Affairs and
Consumer Protection**

Dear Ms. Escareno:

Enclosed herewith is a copy of the fully executed On-Line Access Agreement between the Illinois Secretary of State and the City of Chicago, Department of Business Affairs and Consumer Protection.

This agreement is for obtaining limited driving abstract information from the Driver Services Department, and limited vehicle data from the Vehicles Services Department, of the Office of the Illinois Secretary of State. This agreement will expire on May 29, 2021.

I have also enclosed the Driver's Privacy Protection Act. Please distribute a copy to each employee who will be granted access to Illinois Secretary of State information.

Sincerely,

A handwritten signature in cursive script, reading "Irene Lyons".

Irene Lyons
General Counsel

IL:bg
Enclosure

**ON-LINE ACCESS AGREEMENT
BETWEEN
ILLINOIS SECRETARY OF STATE
AND
THE CITY OF CHICAGO, DEPARTMENT OF BUSINESS AFFAIRS AND CONSUMER PROTECTION
FOR RETRIEVING COMPUTER STORED INFORMATION**

WHEREAS, the City of Chicago, Department of Business Affairs and Consumer Protection, with its principal address at 2350 West Ogden Avenue, Second Floor, Chicago, Illinois 60608 ("Seeker"), seeks to obtain information maintained on the computer files of the Driver Services Department of the Office of the Secretary of State of Illinois, with its principal address at the Driver Services Department, 298 Howlett Building, Springfield, Illinois 62756 and of the Vehicle Services Department of the Office of the Secretary of State of Illinois, with its principal address at the Vehicle Services Department, 312 Howlett Building, Springfield, Illinois 62756 (collectively referred to as "SOS"), pertaining to one or more groups of files described in Section 1 Computer Access;

WHEREAS, Seeker is entitled to certain information maintained in such files which is now available by a manual search of the SOS records for purposes as outlined in Exhibit A and in accordance with the Federal Drivers Privacy Protection Act (18 USC 2721, et. seq.) and other applicable laws;

WHEREAS, the files prescribed in Section 1, Computer Access are "unprotected" in that any party possessing the required access code can obtain virtually all information contained in the files;

WHEREAS, the SOS has decided to grant Seeker retrieval access to these files by on-line access, subject to certain access code security requirements;

NOW THEREFORE, in consideration of the foregoing premises, the mutual agreements of the parties, and other consideration, the receipt and adequacy of which are hereby acknowledged, it is hereby agreed by and between Seeker and SOS, that the following terms and conditions shall control the agreed access to computer files:

1. COMPUTER ACCESS:

SOS will provide on-line access to Seeker seven days a week. Seeker will be authorized to access the following database files ONLY:

From the Driver Services Department: Driver abstracts which are a documented record of only current driver's license number issuance information, convictions, and orders entered revoking, suspending or canceling a driver's license or privilege. All other information shall remain confidential and will not be available to Seeker.

From the Vehicle Services Department: Vehicle title and registration data limited to name, address, and vehicle make, model, license plate and vehicle identification number.

2. FEES AND COMPUTER EQUIPMENT:

Seeker will be responsible for and acknowledges the following:

- a. Obtaining and maintaining access to the Internet that is capable of VPN (Virtual Private Network) traffic. SOS will levy no charges for the communications portion of this agreement.
- b. Obtaining a workstation capable of supporting the necessary access software. Any software needed for access with the exception of that specified in 2d below will NOT be provided by the Secretary of State's office. Examples of access software include a Terminal Emulator, such as an IBM's PCOM or Zephyrsofts Passport PC to host software. While there are many emulators available and Seeker is free to use whatever it chooses, SOS will only support the (2) mentioned options. Another access example is a custom application that communicates via IPSockets or MQSeries. This option is typically considerably more expensive than Emulation, but may be required by the application being accessed. The access software required is determined by the application being accessed, not by this Agreement. SOS Department of Information Technology technical staff must be contacted for details.
- c. SOS will assist with setup via telephone; however, the Seeker is responsible for the client workstation and dealing with its Internet provider should VPN traffic be blocked, intentionally or unintentionally. SOS will attempt to utilize a digital certificate for authenticating to the VPN. Digital certificates are provided free of charge. However, due to technical reasons or requirements determined by SOS, the Seeker may be required to obtain a "Secure-ID" token. A "Secure-ID" token is a device that displays a number that changes every 60 seconds, is synchronized with Springfield, and like the digital certificate, is used for authentication. The cost of a token will be approximately \$100 for three years. Alternatively, a point to point VPN tunnel (requires firewall and/or router at Seeker's location) may be used in place of the digital certificate or "Secure-ID" token client arrangement if the Director of the Department of Information Technology determines proper security procedures are in place in the Seeker's network. This determination will be made solely at the discretion of the Director of the Department of Information Technology. If a VPN tunnel is utilized, the number of devices allowed to use the tunnel shall be kept to a minimum. The maximum number will be determined at the time of the initial VPN setup. The details of the connection, including the "shared secret" will be determined at the time the connection is established. The "shared secret" may be changed by either party on short notice by voice contact between technical personnel. At a later date, SOS may replace the "shared secret" with a digital certificate.
- d. SOS will provide the VPN client (Cisco), if necessary. SOS assumes no responsibility for this software. If a point to point VPN tunnel is utilized, this tunnel must be built on and be compatible with existing SOS VPN equipment (currently CICSOSA Firewall). Additionally, any use of a point to point VPN tunnel requires, at a minimum, 3DES encryption. Conflicts with other applications may require a dedicated workstation. Seeker will not redistribute or take client software outside the United States (a Cisco requirement).
- e. SOS cannot and will not provide support for any emulator other than Zephyrcorps Passport or IBM's PCOMM.

- f. Due to the complexities of machine configurations and software interactions, it may be necessary to dedicate a workstation to SOS host access. Seeker is cautioned to test the installation of the required software before loading the software on its productions machines.
- g. The client software utilized will vary depending upon the access required and the security of the devices being used for access. In order to be permitted simultaneous access to the SOS network and other Internet resources, the Seeker must demonstrate that it has implemented security measures; otherwise, the client software will allow access only to SOS. In order to access other Internet resources, the client software will have to be terminated and then restarted when access is again desired.

3. COMPUTER SECURITY:

- a. Seeker shall take any and all lawful measures necessary to prevent the unauthorized use and disclosure of SOS information and to prevent unauthorized persons or entities from obtaining or using such information. Seeker shall be liable for any unauthorized use and disclosure of SOS data. This includes, but is not limited to: data breaches, accessing the database(s) without authority, allowing anyone not a party to this Agreement to access the database(s) or to view SOS information or altering any existing SOS information in any form. Seeker must immediately report any unauthorized use or misuse of SOS information, including any breach of Seeker's security system that may involve SOS information, to SOS by contacting the Secretary of State Department of Information Technology (217/558-0049) and the Office of the General Counsel (217/785-3094).
- b. If a data security breach occurs during the term of this Agreement, Purchaser shall allow a forensics expert selected by SOS to conduct a full and thorough investigation and report his or her findings at Purchaser's expense. Purchaser shall cooperate fully with said forensic expert during his or her investigation and shall provide him or her with all documentation, access or other assistance the expert shall deem necessary. Purchaser agrees SOS shall have full and unfettered access to the results of any such investigations.
- c. SOS will provide Seeker, in documents separate from this Agreement, with an agency code for VPN access. Seeker will be responsible for the security of this information, including the prevention of any unauthorized use. Ultimately, Seeker shall be responsible for any unauthorized use. Seeker acknowledges that SOS has the authority to change the requirements for accessing the system as technological, fiscal, security or other considerations dictate. SOS agrees to provide Seeker with as much prior notice of such changes as is practicable. Upon termination of this Agreement, Seeker shall immediately return to SOS all documents concerning access to SOS data, whether tangible, electronic or otherwise, in its custody, possession or control, and shall immediately cease using such access.
- d. Prior to execution of this Agreement and upon request, Seeker shall provide to SOS the names, addresses and phone numbers of all persons responsible for managing SOS data

or otherwise executing the provisions of this Agreement on behalf of the Seeker. SOS must issue an individual RACF ID to every officer and employee of Seeker before the officer or employee may access SOS data. Under no circumstances may officers or employees of Seeker share a RACF ID. When the Seeker no longer employs an officer or employee, Seeker must immediately notify SOS so that the RACF ID of that officer or employee can be terminated. Breach of the provisions of this paragraph shall be deemed a material breach and will result in this Agreement being terminated by SOS.

- e. This Agreement authorizes Seeker only to retrieve data from the database(s) set forth in Section 1. Computer Access. Seeker may not enter any information on any SOS file, nor may Seeker alter, or attempt to alter, any existing SOS file in any form.
- f. This Agreement authorizes the SOS or its representatives access to Seeker's system to audit, verify and assess security controls. Failure to provide adequate security controls is a material breach and cause for immediate termination.
- g. SOS security policies and any data security standards contained therein, as amended, shall be incorporated into this Agreement by reference. Seeker shall also adhere to the International Standards Organization (ISO) 27001 and ISO 27002. Upon notice to Seeker, SOS reserves the exclusive right to add and/or modify these and other data security requirements contained in this Agreement at any time during its term.
- h. As a condition precedent of this contract, Seeker agrees to complete the SOS Network Security Assessment, if required by SOS and to return same to SOS prior to the execution of this contract.

4. DATA MINING PROHIBITIONS:

- a. Seeker agrees to refrain from any type of data mining or web mining of SOS data.
- b. Prohibited data mining/web mining includes, but is not limited to, use of website copying software, web data pre-processing, creation of web metrics and mathematical models, web log analysis, static and dynamic visitor profiling, intelligent information retrieval, hyperlink analysis, use of spider, crawl or bot programs (vertical search engines), web usage mining, web structure mining, web content mining, data/information extraction, web information integration and schema matching, knowledge synthesis, segmenting, noise detection, use of topic-sensitive PageRank software, use of filtering techniques, meta-search engines, or any other type of automated search of information that goes beyond keyword extraction.
- c. Violation of this section is considered a material breach and will result in termination of online access.
- d. Data/Web mining is considered "Computer Tampering," a criminal act under the Illinois Criminal Code. A person who commits the offense of "Computer Tampering" is guilty of a Class 4 Felony. 720 ILCS 5/17-51.

5. USE OF INFORMATION:

- a. Seeker agrees that it will obtain the data from SOS on an "AS IS" basis. Seeker acknowledges that SOS compiles the data as required by statute for its own public purposes, and that by providing such data to Seeker pursuant to this Agreement, SOS is providing only access convenient to Seeker. SOS assumes no responsibility for the accuracy of the data and disclaims any liability for damages, costs, and/or expenses, including, without limitation, consequential damages, arising or resulting from any inaccurate data.
- b. Seeker represents that this request for information is in accordance with Federal and Illinois law. Seeker has furnished a certified statement (in the form of a sworn and notarized affidavit) setting forth the specific uses to be made of the data received from SOS. This certified statement shall be subject to the approval of SOS and shall be incorporated into this Agreement as Exhibit A. Seeker agrees neither to deviate from nor to alter the certified statement of specific uses without the prior express written consent of SOS. This Agreement authorizes SOS or its representative to audit Seeker, including any and all computer systems and documents, to verify that the data is being used only in accordance with the approved certified statement. *jm Lyons* *PLC*
- c. Seeker agrees that the data received ~~in its original form~~ will not be made available to other persons, firms, corporations, partnerships, members of the public, persons outside the employ or direct control of the Seeker or other entities, other than as indicated in the certified statement of use, without the prior express written consent of SOS.
- d. Pursuant to 92 Illinois Administrative Code 1002.60, should Seeker disclose any personal information obtained from SOS in any manner allowed under this Agreement, Seeker shall, for a minimum of five (5) years, keep records identifying each person or entity that received such information and the permitted purpose for which the information was disclosed. Seeker will make said records available to SOS upon request by SOS.
- e. No person shall be allowed to access SOS's computer system or shall be allowed access to data obtained from SOS's computer system for reasons outside of the Seeker's intended and legitimate use of such information under this Agreement, as identified in the approved certified statement of uses.
- f. While some of the data contained in such files is considered public information, some of the data to which Seeker is entitled is considered personally identifying information, the dissemination of which is limited by federal and state law, including the Federal Drivers Privacy Protection Act, 18 USC 2721 et. seq. Seeker acknowledges that the improper dissemination of personally identifying information is a violation of the Federal Drivers Privacy Protection Act and that any individual who violates this Act is subject to criminal prosecution, fines and civil penalties of \$2,500 for each improper disclosure of information. Thus, all information whether displayed on the screen or in printed form is for the EXCLUSIVE use of Seeker and shall not be provided to anyone not a party to this Agreement except as provided in the Certified Statement of Use(s). Seeker agrees that each of the employees designated by Seeker who will be granted access to SOS information will be given a copy of the Driver's Privacy Protection Act describing the

limitation on the dissemination of this information and of the civil and criminal penalties for violating the Driver's Privacy Protection Act. Each designated employee shall certify, in writing, compliance with the Driver's Privacy Protection Act. Said Certification and Driver's Privacy Protection Act are attached for Seeker to copy and disseminate to all designated employees who will have access to said confidential information. Signed copies of the Certification shall be returned to: Office of the General Counsel, Illinois Secretary of State, 298 Howlett Building, Springfield, Illinois 62756. Access will not be granted until all designated employees of Seeker have signed and returned the Certification to the Illinois Secretary of State General Counsel.

- g. All members of the public must, by law, purchase copies of abstracts for their own use from SOS as outlined in 625 ILCS 5/2-123 and 92 Illinois Administrative Code 1002.
- h. Seeker shall adhere to the Data Processing Confidentiality Act. 30 ILCS 585 et. seq. Seeker agrees not to use, furnish, or otherwise make available drivers, vehicles or title lists or any other data supplied pursuant to this Agreement for commercial solicitation purposes, to contact individuals for advertising, offering for sale, marketing or sale of products or services; or identifying potential employees, except for the United States Armed Forces; or to update, enhance, or verify any information which may then be sold, offered or otherwise distributed to any user to directly or indirectly use such information to contact individuals for advertising, offering for sale, marketing or sale of products or services as set forth by Title 92, Illinois Administrative Code, Chapter II, Section 1002.42. A violation of this provision shall result in the SOS's denial of sale of information to the Seeker for a term of five (5) years.
- i. Seeker agrees to properly and timely dispose of the materials containing personal information in a manner that renders the personal information unreadable and undecipherable, in accordance with the Personal Information Protection Act. 815 ILCS 530. Furthermore, a violation of the Personal Information Protection Act may subject Seeker to monetary and civil penalties not to exceed \$50,000 for each instance. 815 ILCS 530/40(a).
- j. Seeker acknowledges that a violation of the Personal Information Protection Act constitutes an unlawful practice under the Consumer Fraud & Deceptive Business Practices Act. (815 ILCS 530/20).
- k. Should Seeker misuse SOS information or have a breach of its security systems that allows unauthorized users access to SOS information, Seeker shall be responsible for any damages and costs SOS incurs in relation to notifying SOS customers of the unauthorized access and/or use of their information.
- l. Seeker agrees to indemnify and hold the SOS, its officers, agents and employees, harmless from and against any and all liabilities, demands, claims, suits, losses, damages, causes of action, fines or judgments, including costs, attorneys' and witnesses' fees, and expenses incident thereto, relating to the unauthorized access to and/or release or misuse due to both 1) the acts or omissions of Seeker, its employees, or agents and 2) a breach of its computer security systems that compromises the security of SOS information. Both shall result in SOS having to notify its customers of the misuse

or compromise of their information and Seeker shall bear all costs and damages associated with said notification and breach.

- m. Breach of any of these provisions contained within this section by Seeker shall be deemed a material breach of this Agreement and shall result in the immediate termination of this Agreement.

6. FORCE MAJEURE:

Seeker acknowledges that SOS agrees to provide computer accessible stored data to Seeker as an accommodation to Seeker. SOS shall not be responsible for any failure to deliver data in a timely manner or at all, in the event that SOS suffers a breakdown of its computer stored information facilities, the failure of transmission equipment, fire, floods, earthquakes, explosions, acts of authority exercised by a public functionary, acts of a public enemy, legislation, governmental regulation or other such circumstances which are difficult to foresee and resist, and which impede the ability of SOS to provide the services described in this Agreement, which shall be known as force majeure. SOS shall notify Seeker of an event of force majeure that may delay or preclude provision of the data contemplated under this Agreement, and shall notify Seeker when such force majeure no longer exists or precludes or delays such provision of data. SOS shall refund any payment made by Seeker for undelivered data; however, SOS shall have no further responsibility or liability to Seeker with respect to such undelivered data.

7. GOVERNING LAW AND JURISDICTION:

This Agreement is subject to the rules outlined in 92 Illinois Administrative Code 1002, and 1030.140, all relevant sections of the Illinois Vehicle Code and all federal laws, including the Federal Drivers Privacy Protection Act, 18 USC 2721 et seq., the Personal Information Protection Act, 815 ILCS 530, Data Processing Confidentiality Act, 30 ILCS 585, and the Fair Credit Reporting Act, 15 USC 1681 et seq. This Agreement shall be interpreted in accordance with the laws of the State of Illinois, U.S.A. Seeker agrees that any dispute arising under this Agreement which cannot be resolved amicably among the parties shall be submitted to the court of competent jurisdiction in the State of Illinois, to which jurisdiction Seeker hereby submits.

8. TERM AND TERMINATION:

- a. Term. The effective date of this Agreement shall be the date set out at the end hereof. This Agreement shall continue in effect until termination by either party pursuant to the terms hereof, or until the breach of any of the terms and conditions of this Agreement, and in particular Sections 3., 4. and 5., or by three (3) years from the effective date set out at the end hereof, whichever comes first.
- b. Termination on notice. The parties shall each have the right to terminate this Agreement without cause upon 5 days prior written notice to the other party.
- c. Additional basis for termination. The SOS shall have the right to terminate this Agreement immediately if, at any time, Seeker shall breach any material provision of this Agreement.

- d. Survival of terms. The terms and conditions of Sections 2. Fees and Computer Equipment, 3. Computer Security, 4. Data Mining Prohibitions, 5. Use of Information, and 7. Governing Law and Jurisdiction and this paragraph are substantive provisions constituting the essence of the Agreement and the obligations of the parties. These provisions shall survive termination of this Agreement unless and until discharged by the parties.

9. NOTICE:

Any and all notices required or permitted to be given under this Agreement shall be in writing and shall be deemed sufficiently made if given by certified or registered mail, postage prepaid, addressed to a party by name at the address first indicated above. Except as specifically provided herein, notices so given shall be deemed made when delivered to the addressee; provided, however, that if delivery of such mail is delayed or not effectuated for any reason other than temporary or permanent loss in, or substantial disruption of, the mails, then such notice shall be deemed to have been made on the 5th business day following the date of deposit in the United States mails. A receipt showing delivery of certified or registered mail, signed by the addressee or its agent or employee, or a written notification given in due course by the postal authority indicating the reason for non-delivery shall be sufficient evidence thereof, respectively. The aforesaid address for service of notice may be changed only by the changing party giving 10 days' notice thereof by certified or registered mail in the manner hereinabove provided, but there shall be no presumption of delivery of such notice of change of address in the absence of actual delivery. Nothing herein contained shall preclude the giving of written notice by any other lawful means.

10. GENERAL:

- a. Integrated Agreement. This Agreement constitutes the final agreement between the parties concerning online access by Seeker to the Computer Stored Information of the SOS and supersedes all previous agreements, promises, representations, understandings and negotiations, whether written or oral, among the parties with respect to the subject matter hereof and shall be binding upon and inure to the benefit of the parties' respective successors.
- b. Assignment. Seeker may not assign any right or obligation hereunder. Any attempted assignment in violation of this provision shall be void and of no effect.
- c. Implementation. Each party hereto agrees to execute such further documents and take such further steps as the other party reasonably determines may be necessary or desirable to effectuate the purposes of this Agreement.
- d. Compliance. Each party hereto shall comply with all applicable laws, rules, ordinances, guidelines, consent decrees and regulations of any federal, state, or other governmental authority.
- e. Waiver. No modification, amendment, supplement to or waiver of this Agreement or any of its provisions shall be binding upon a party hereto, unless made in writing and

duly signed by such party. A failure of or delay by either party to this Agreement to enforce at any time any of the provisions of this Agreement or to require at any time performance of any of the provisions of this Agreement shall in no way be construed to be a waiver of such provision. A waiver by either party of any of the terms and conditions of this Agreement in any individual instance shall not be deemed a waiver of such terms or conditions in the future, or of any subsequent breach of this agreement.

- f. Severability. If any provision(s) or clause(s) of this Agreement, or portion thereof, are held by any court or other tribunal of competent jurisdiction to be illegal, void or unenforceable in such jurisdiction, such provision(s) or clause(s) shall be reformed to approximate as nearly as possible the intent of the parties, and the remainder of the provisions shall not thereby be affected and shall be given full effect without regard to the invalid portion, and to this end such provisions are declared to be severable.
- g. Headings. The descriptive headings of the Sections of this Agreement are inserted for convenience only, and do not constitute a part of this Agreement.
- h. Counterparts. This Agreement may be executed in two or more counterparts, each of which shall be deemed to be an original but all of which together shall constitute one and the same instrument.
- i. Fiscal planning. The continuation of this contract and the obligations of the State are contingent upon the appropriation by the legislature or federal funding source of sufficient and appropriate funds to fulfill the requirements of the contract. If sufficient funds as determined by the State are not appropriated, the contract shall terminate on the first date in any fiscal year on which sufficient funds are no longer available. The State will give 30 days or as much notice as possible of an appropriation issue.
- j. Felony Conviction/Criminal Background Check. Seeker certifies that neither Seeker nor any employee or officer of Seeker has been convicted of a felony, or, if so convicted, at least five years have passed since completion of sentence as of the effective date of this Agreement. (30 ILCS 500/50-10)

THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK.

IN WITNESS WHEREOF the Parties hereto have executed this Agreement on the dates attested to below:


DATE: 5/17/18

CITY OF CHICAGO, DEPARTMENT OF BUSINESS AFFAIRS
AND CONSUMER PROTECTION

By: 
Rosa Escareno
Commissioner

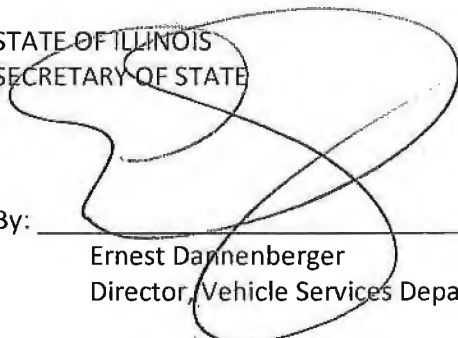
DATE: 5-29-18

STATE OF ILLINOIS
SECRETARY OF STATE

By: 
Michael J. Mayer
Director, Driver Services Department

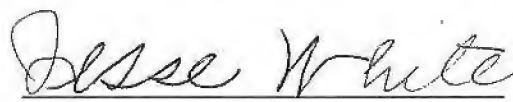
DATE: 5/30/18

STATE OF ILLINOIS
SECRETARY OF STATE

By: 
Ernest Dannenberger
Director, Vehicle Services Department

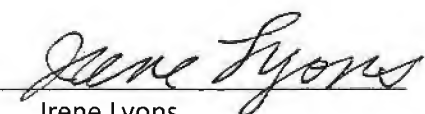
DATE: 6/1/18

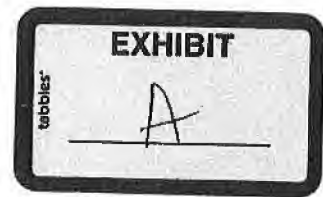
STATE OF ILLINOIS
SECRETARY OF STATE


JESSE WHITE
SECRETARY OF STATE

Reviewed for Legal Sufficiency:

Date: 6/1/18

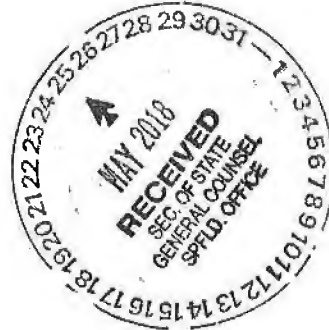
By: 
Irene Lyons
General Counsel
Illinois Secretary of State's Office



DEPARTMENT OF BUSINESS AFFAIRS AND CONSUMER PROTECTION
CITY OF CHICAGO

April 17, 2018

Pamela Wright
Office of the General Counsel
298 Howlett Building
Springfield, Illinois 62756



Dear Ms. Wright:

In the spirit of inter-agency collaboration and shared regulatory mission, the City of Chicago's Department of Business Affairs and Consumer Protection (BACP) respectfully requests direct, real-time, on-line access to the driver and vehicle databases maintained by the Illinois Secretary of State (SOS). BACP makes this request to gain access to information including, but not limited to, vehicle plates, VIN numbers, and driver's license numbers. We also request access to full driver's license abstracts because we license taxis, liveries, valets. We also regulate Transportation Network Providers (TNPs) under Municipal Code of Chicago 9-115. Abstracts would help us determine whether or not these service providers are using drivers with negative driving records, as negative driving records can be grounds for license revocation by BACP.

BACP's Business and Compliance Enforcement division (BCE) is a regulatory agency staffing sworn peace officers that investigates alleged violations of the Municipal Code of Chicago. Our investigations result in citations and hearings. The accuracy and efficiency in obtaining these records are essential.

BACP's BCE completes rigorous background checks needed for all Tobacco Vendor, Liquor, and Public Place of Amusement license applications.

BACP's BCE receives cases where consumer fraud has been established, but where information on the defrauder may be limited to a license plate and vehicle.

BACP's BCE regulates businesses that operate from a vehicle and the public way and conducts rigorous background checks on those business owners.

BACP's BCE investigates complaints involving motor vehicle repair and auto sales.

BACP's Public Vehicles division (PV) is the regulator for the taxi cab industry in the City of Chicago. As such, the department investigates a large volume of consumer complaints (over 50,000 per year). Each investigation requires the above listed information to make a positive identification of vehicle owners.

BACP's PV conducts real time analysis required to verify the information drivers provide to the City in the course of taxi cab registration, medallion transfers, and MPEA Airport Departure Tax applications.

Pamela Wright
April 17, 2018
Page two

BACP's PV conducts truck weight enforcement and must ascertain the true ownership and history of identified vehicles.

BACP staff authorized to access the requested SOS databases will comply with, and acknowledge the ramifications of misuse of, the Federal Drivers Privacy Protection Act (18 USC 2721) and all other applicable laws, rules and regulations. A listing containing the name, title, work phone number and address of those who require this access is enclosed herewith.

Thank you for your assistance in increasing the accuracy and efficiency of our investigations, and also in joining us to help protect the public from unfair and unscrupulous business practices.

Sincerely,



Rosa Escareno
Commissioner

Enclosure
RE:rlc

Sworn to and subscribed before me this 24th day of May A.D. 2018






DEPARTMENT OF BUSINESS AFFAIRS AND CONSUMER PROTECTION
CITY OF CHICAGO

**BUSINESS AFFAIRS AND CONSUMER PROTECTION
BUSINESS COMPLIANCE ENFORCEMENT & PUBLIC VEHICLES EMPLOYEES
REQUIRING ACCESS TO
ILLINOIS SECRETARY OF STATE DRIVER AND VEHICLE DATABASES**

USERS WITH CURRENT ACCESS:

1. Nicholas Giannoules, Manager of Business Compliance, (312) 743-9103 (BCE)
2. Adam Weller, Supervisor of Business Compliance, (312) 743-1429 (BCE)
3. Javier Ortiz, Manager of Business Compliance, (312) 746-8673 (PV)
4. Joseph Sneed, Supervisor of Business Compliance, (312) 743-9106 (BCE)
5. Dennis Guillermo, Manager of Business Compliance, (312) 743-1428 (BCE)

The business address for all users listed above is 2350 West Ogden Avenue, Chicago, Illinois 60608.

Federal Drivers' Privacy Protection Act

(Title 18 U.S.C. § 2721 et seq.)

§ 2721. Prohibition on release and use of certain personal information from state motor vehicle records

(a) **In general.** A state department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity:

- (1) personal information, as defined in 18 U.S.C. § 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section; or
- (2) highly restricted personal information, as defined in 18 U.S.C. § 2725(4), about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies, except uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9): *Provided*, That subsection (a)(2) shall not in any way affect the use or organ donation information on an individual's driver's license or affect the administration of organ donation initiatives in the states.

(b) **Permissible uses.** Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring or motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. § 1231 et seq.), the Clean Air Act (42 U.S.C. 7401 et seq.), and chapters 301, 305, and 321-331 of title 49 [49 U.S.C. § 30101 et seq., 30501 et seq., 32101 et seq.-33101 et seq.], and, subject to subsection (a)(2), may be disclosed as follows:

- (1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a federal, state or local agency in carrying out its functions.
- (2) For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.
- (3) For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only –
 - (A.) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
 - (B.) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
- (4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a federal, state or local court.

§ 2722. Additional unlawful acts

- (a) Procurement for unlawful purpose.** It shall be unlawful for any person knowingly to obtain or disclose personal information from a motor vehicle record for any use not permitted under section 2721(b) of this title [18 U.S.C. § 2721(b)].
- (b) False representation.** It shall be unlawful for any person to make false representation to obtain any personal information from an individual's motor vehicle record.

§ 2723. Penalties

- (a) Criminal fine.** A person who knowingly violates this chapter [18 USC § 2721 et seq.] shall be fined under this title.
- (b) Violations by state department of motor vehicles.** Any state department of motor vehicles that has a policy or practice of substantial noncompliance with this chapter [18 USC § 2721 et seq.] shall be subject to a civil penalty imposed by the Attorney General of not more than \$5,000 a day for each day of substantial noncompliance.

§ 2724. Civil action

- (a) Cause of action.** A person who knowingly obtains, discloses or uses personal information from a motor vehicle record for a purpose not permitted under this chapter [18 USC § 2721 et seq.] shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court.
- (b) Remedies.** The court may award-
 - (1) actual damages, but not less than liquidated damages in the amount of \$2,500;
 - (2) punitive damages upon proof of willful or reckless disregard of the law;
 - (3) reasonable attorneys' fees and other litigation costs reasonably incurred; and
 - (4) such other preliminary and equitable relief as the court determines to be appropriate.

§ 2725. Definitions

In this chapter [18 U.S.C. § 2721 et seq.]—

- (1) "motor vehicle record" means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles;
- (2) "person" means an individual, organization or entity, but does not include a state agency thereof;
- (3) "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver information number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status;
- (4) "highly restricted personal information" means an individual's photograph or image, social security number, medical or disability information; and
- (5) "express consent" means consent in writing, including consent conveyed electronically that bears an electronic signature as defined in § 106(5) of Public Law 106-229 (15 U.S.C. § 7006(5)).